Takes the place of EP1064755 (Art.158 of the EPC)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/00

A2

(11) International Publication Number: **WO 99/46692**

(43) International Publication Date: 16 September 1999 (16.09.99)

(21) International Application Number: PCT/US99/04699

(22) International Filing Date: 3 March 1999 (03.03.99)

(30) Priority Data:
09/042,338 13 March 1998 (13.03.98) US

(71) Applicant: OMNES [US/US]; Suite 400, 5599 San Felipe, Houston, TX 77056 (US).

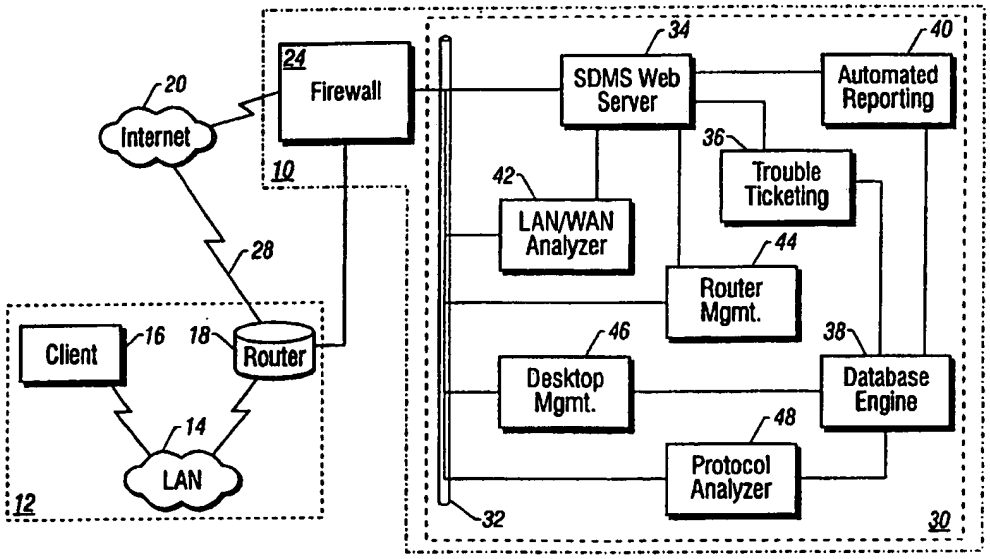
(72) Inventor: CUNNIHAM, Chris, M.; 4520 Pin Oak, Bellaire, TX 77401 (US).

(74) Agents: OSHA, Jonathan, P. et al.; Rosenthal & Osha L.L.P., Suite 4550, 700 Louisiana Street, Houston, TX 77002 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: PROVIDING NETWORK SERVICES THROUGH A COMMON INTERFACE



(57) Abstract

Information is provided to a customer whose computer network is administered remotely by a provider of network administration services, some of which are carried out by dedicated service machines executing special–purpose programs in a computer network maintained by the service provider. A graphical computer interface allows the customer to request, via computer, information about the customer's network from any of the dedicated service machines. The requested information then is retrieved from an appropriate one of the dedicated service machines and is displayed to the customer via the graphical computer interface.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

PROVIDING NETWORK SERVICES THROUGH A COMMON INTERFACE

Cross Reference To Related Applications

This application is related to and incorporates by reference U.S. application 09/039,167, filed on March 13, 1998, by James M. Sullivan and James A. Keddie and entitled "Providing Secure Access to Network Services."

Background

Most large business entities use some form of local or wide area computer network to conduct daily business. Many of these entities do not want to maintain large computer staffs and therefore delegate most network management responsibilities to an off-site network management provider. In general, these network management providers maintain full control over the customer's network. As a result, information about the customer's network, such as the utilization patterns and overall health of the network, and information about the service performance of the network management provider, is not readily available to the customer. The customer generally must request this information from the network management provider and await the delivery of a report.

Summary

In one aspect, the invention relates to the remote administration of a customer's computer network by a provider of network administration services, such as a trouble ticketing service or a network monitoring service, some of which may be carried out by dedicated service machines executing special-purpose programs in a computer network maintained by the service provider. A graphical computer interface allows the customer to request, via

computer, information about the customer's network from any of the dedicated service machines. The requested information then is retrieved from an appropriate one of the dedicated service machines and is displayed to the customer via the graphical computer interface.

In some embodiments, the graphical computer interface may be presented in a format that allows viewing through an off-the-shelf browser application. The graphical computer interface may be presented by executing a program on a network server computer, which in turn may be configured to deliver the customer's request to the appropriate service machine. One instance of the program may be executed for each customer accessing the service provider's network, and a customer-specific version of the graphical computer interface may be presented to each customer.

In addition, the network server computer may be configured with a unique IP address for each customer capable of accessing the service provider's network, and each IP address may be preassigned to only one customer. Each IP address may represent a TCP/IP stack in the network server computer.

Each embodiment of the invention may provide any one or more of several advantages. For example, the customers of a network management service provider may access a wide variety of information about their local networks through an easy-to-use, Web-based interface viewed through an off-the-shelf browser. The customers can access much of the information almost immediately via computer, without having to submit requests to human operators and await human action for responses to the requests. The customers also do not need to purchase or even understand the hardware and software components used to provide the network management

services. In short, the owner of a computer network can outsource essentially all network management responsibilities without forfeiting quick and easy access to information about the network. The network owner also can receive quick and easy-to-understand reports on the service provider's performance.

Other embodiments and advantages will become apparent from the following description and from the claims.

Brief Description of the Drawings

FIG. 1 is a schematic diagram of computer network that provides network services to a remote client computer.

FIG. 2 is a functional block diagram of network server computer through which the client computer accesses the network services.

FIG. 3 is a schematic diagram of hardware and software components of the network server computer.

FIG. 4 is a directory structure under which the network server computer may store the software components required to provide the network services.

FIG. 5 is a view of a graphical user interface through which a user of the client computer can access the network services.

Detailed Description

Referring to FIG. 1, a network service provider maintains a computer network 10 that provides network services to one or more customers at remote customer sites 12. These services together form an integrated management system, through which the network service provider's customers can receive complete network support and management through a single, remote point of contact, as discussed below. Typically, each customer site 12 houses a

local area network (LAN) 14, connected to which is at least one client computer 16 capable of accessing the network services through the provider's computer network 10. Each customer site 12 also typically includes a router 18 that governs the flow of traffic between the customer's LAN 14 and any network outside the customer site 12, such as the service provider's network 10 and the Internet 20.

The customer can connect to the provider's network 10 in several ways, including a direct link 26 to the network 10 through a frame relay (FR), Point-to-Point Protocol (PPP), or Integrated Services Digital Network (ISDN) connection, and an indirect link 28 via the Internet 20. All traffic between the customer's site 12 and the provider's network services must pass through a firewall 24, which guarantees each customer secure access to the network services and which protects the service provider's network from unwanted intrusion by its customers and by other remote entities. Copending U.S. patent application 09/039,167, filed on March 13, 1998, by James M. Sullivan and James A. Keddie (incorporated by reference), describes a network architecture through which the network service provider's customers may access the network services securely. In that application, the firewall 24 is implemented as a static routing policy distributed among four server computers, one of which governs all access to the network services, including access from within the provider's network 10, and the rest of which govern access to the provider's network 10 by its customers.

The network service provider may provide a wide variety of network management services, including an action request system, through which a customer can submit requests for solutions to problems related to its LAN 14 and to individual computers connected to the LAN 14; a network

monitoring service, which gathers and provides information about the performance of the customer's LAN 14; service utilization reports, which provide information indicating how the customer is using the network services; an electronic mail archive that preserves correspondence between the customer and the network service provider; a bulletin board on which the customer can post information to the users of its LAN 14 and the network service provider can post notices to the customer; a purchase requisition service, through which the customer can purchase hardware and software from the network service provider; and an on-line help service. These services are provided, at least in part, by a subnetwork 30 of computers ("service machines") linked to the firewall 24 through a connection such as an Ethernet cable 32 or a token ring. Each of the computers in the subnetwork 30 may be, *e.g.*, a network server computer configured to implement one of the network services or a network component needed to provide the services.

The subnetwork 30 includes an interface server computer, or "web server" 34, that provides the interface through which the service provider's customers can access all of the network services. The web server 34 may be implemented, *e.g.*, as a Netscape Enterprise Server running an executable program that allows the customer to access all of the services through a single, hypertext transfer protocol (http) based interface, which the customer may view through an off-the-shelf web browser, such as Netscape Navigator or Microsoft Internet Explorer. The web server 34, including the customer interface, is described in more detail below.

The action request service is provided by a trouble ticketing server 36 running a trouble ticketing program, such as Remedy Corporation's "Action Request System" (AR

System) software. A program such as Remedy's "ARWeb" interface may be used to provide the communication interface between the web server 34 and the trouble ticketing server 36. The trouble ticketing server 36 allows each of the network service provider's customers to submit trouble tickets requesting assistance from the network service provider and to generate inquiries into the progress of those trouble tickets. The action request server 36 also generates statistical information about each customer's utilization of the action request service. All of the information generated by the trouble ticketing server 36 is stored in a database engine 38, such as a Sybase engine. The trouble ticketing server 36 and the database engine 38 may employ, *e.g.*, Microsoft's "Open Database Connectivity" (ODBC) standard to transmit data to each other.

An automated reporting server 40 running, *e.g.*, Seagate Software's "Crystal Info" application gathers information from the database engine 38 and generates periodic (*e.g.*, daily) reports for each customer. The automated reporting server 40 may use, *e.g.*, the ODBC protocol to retrieve information from the database engine and the file transfer protocol (ftp) to deliver the reports to the web server 34. The web server 34 in turn provides the reports to the customer through the http interface. The reports generated by the automated reporting server 40 may include information such as the number of trouble tickets submitted by a customer on a given day, the amount of time taken to resolve these tickets, and the number of tickets submitted by a given department within the customer's organization.

The network monitoring service is distributed among two computers, a network analyzer server 42 running, *e.g.*, Concord Communications' "Network Health" software, and a

router management server 44 running, *e.g.*, Cabletron Systems' "Spectrum Enterprise Manager" software. Via the Ethernet connection 32 to the firewall 24, the network analyzer 42 utilizes Simple Network Management Protocol (SNMP) polling of the customer's LAN 14 to gather information about the flow of information through certain devices that have been registered with the network analyzer 42, including bridges, routers and switches in the customer's LAN 14. The "Network Health" application running on the server 42 uses this information to analyze usage trends in the LAN 14, to evaluate the overall health of the LAN 14, and to identify components in the LAN 14 that have been affected by events such as errors and high bandwidth utilization. The application generates reports that, among other things, indicate the weekly, daily, and hourly traffic volumes of registered devices in the LAN 14, identify the devices that have experienced the highest traffic volumes and those have undergone the greatest changes in traffic volume, and indicate the bandwidth utilization for each registered device in the LAN 14. The network analyzer 42 delivers the reports directly to the customer, bypassing the web server 34, as discussed below.

The router management server 44 also conducts SNMP polling to gather information from the customer's LAN 14. Using Cabletron's "Spectrum Enterprise Management" application, this server 44 recognizes when a problem is occurring in the customer's LAN 14, determines precisely where the problem is occurring, identifies a probable cause of the problem, and generates an alarm message that reports all of this information and that suggests an action to resolve the problem. The server 44 updates the alarm information periodically, *e.g.*, every thirty seconds, to ensure that problems in the customer's LAN 14 are detected

quickly. The server 44 uses Cabletron's "AlarmWeb" application to provide the alarm information to the web server 34.

A desktop management server 46 also links to the firewall 24 through the Ethernet connection 32. This server 46, which runs one or more network management applications such as Microsoft's "System Management Server" (SMS) and Compaq's "Insight Manager" (CIM), uses SNMP polling to gather information about the desktop configuration of each client computer 16 at the customer site 12. The server 46 stores this information in the database engine 38, where the network service provider's personnel can access the information for use in solving the customer's problems.

A protocol analyzer server 48 polls each customer's LAN 14 for information about traffic in the LAN 14. For example, the protocol analyzer server 48 may use NetScout's protocol analyzer application to retrieve protocol distribution information from NetScout probes embedded in the customer's LAN 14. The protocol analyzer 48 stores this information in the database engine 38 for access by the customer and the network service provider.

Referring to FIG. 2, the web server 34 may be a standard programmable computer, such as a Sun UltraSparc workstation, having a central processing unit (CPU) 50 and system memory coupled to a system bus 56. The system memory may include both random access memory (RAM) 52 and non-volatile memory, *e.g.*, read-only memory (ROM) 54. An input/output (I/O) interface 58 coupled to the system bus 56 and to an I/O bus 60 facilitates the flow of data between the CPU/system memory and various input and output devices, including a fixed storage device such as a hard disk 62. The hard disk 62 typically includes several executable programs, each of which may be loaded into RAM 54 to program

the computer 34 to perform certain predefined functions. One of these programs is a network server application, such as Netscape's "Enterprise Server" program 64, which enables the computer to function as a Web server. The hard disk 62 also contains a "web interface" program 66, which provides the interface through which the service provider's customers access the network services. The communication programs "ARWeb" 68 and "AlarmWeb" 70 also are stored on the hard disk 62. As discussed above, these programs, when loaded into system memory, allow the web server 34 to communicate with the trouble ticketing server 36 and the router management server 44, respectively. The hard disk 62 also stores one or more script files 74 that allow the web server 34, while executing the web interface program 66, to create and maintain a unique "web site" for each of the service provider's customers. As discussed below, the web site associated with a customer allows that customer, and only that customer, to access the network services.

Referring also to FIG. 3, the web server 34 maintains a unique TCP/IP stack (S1 ... Sn) for communication with each customer and another TCP/IP stack (Sx) for communication with all of the service machines in the subnetwork 30 (FIG. 1). The firewall 24 maintains information linking each of the customer-specific TCP/IP stacks (S1 ... Sn) with the IP address of the router 18 at a corresponding customer site 12. Upon receiving a query from a customer site 12, the firewall 24 determines the IP address of the customer site 12 and then forwards the request directly to the corresponding TCP/IP stack in the web server 34. The firewall 24 also ensures that all traffic flowing from a customer-specific TCP/IP stack in the web server 24 is routed only to the corresponding customer site 12.

The web server 34 creates a unique web site, or web server process (WS1 ... WSn), for each customer by running one copy of a network server application, such as Netscape's "Enterprise Server" application 64, for each customer. Each web server process is given unique user, process and group identifiers (UID, PID and GID) to ensure that only files associated with that web process and the corresponding customer can be accessed in processing a query from the customer site. The UID and GID are determined by a unique customer account, *e.g.*, a Unix account (U1 ... Un), that is established when the customer's web site is added to the web server. Each Unix account includes a unique web name and password identifying the customer associated with the account. The customer accounts are used only by the processes running on the web server 34 and are not visible to the customers.

The web server 34 runs one instance of an alarm application, such as Cabletron's "AlarmWeb" application, for each customer having access to the router management service. If "AlarmWeb" is used, each instance of the application is launched as an AlarmWeb process (AW1 ... AWn) when the web server 34 is first booted up. Once running, each AlarmWeb process periodically (*e.g.*, once per minute) retrieves, from the router management server via the network services TCP/IP stack (Sx), two files containing alarm information for the corresponding customer site. The AlarmWeb process then stores the files in the web server, *e.g.*, on the hard disk or in memory. One of the files, an "alarms.HTML" file, provides a description of each alarm that has occurred in the customer's LAN; the other file, a "totals.HTML" file, indicates the total number of alarms that have occurred in the customer's LAN. The AlarmWeb process uses the identifiers defined in the corresponding

customer account to retrieve the "alarms.HTML" and "totals.HTML" files from the router management server, which itself periodically updates the information in the files by SNMP polling the customer site, as discussed above. Upon receiving a customer query from a TCP/IP stack, the corresponding web process delivers the query to the associated AlarmWeb process, which in turn retrieves the stored files and delivers the information contained in them to the corresponding customer.

The web server 34 runs only one instance of Remedy's "ARWeb" program, *i.e.*, one ARWeb process, to access information in the trouble ticketing server, regardless of how many customers subscribe to the trouble ticketing service. The web server ensures security by maintaining for each customer a unique ARWeb account (A1 ... An), which the web server must reference to access information in the trouble ticketing server. As with the Unix accounts described above, each ARWeb account includes a unique user name and password identifying the associated customer. The ARWeb accounts are not visible to the customers.

Upon receiving a trouble ticket from a customer-specific TCP/IP stack (S1 ... Sn), the corresponding web server process (WS1 ... WSn) accesses the ARWeb (A1 ... An) account for the customer and then forwards the trouble ticket to the ARWeb process (AR). The ARWeb process then delivers, via the network services TCP/IP stack (Sx), the trouble ticket to the trouble ticketing server, which in turn logs the ticket in the database engine. The information in the database engine is updated periodically to reflect progress made by the network service provider in processing the problem identified in the trouble ticket.

Upon receiving an inquiry about the status of trouble tickets from a customer through the corresponding

TCP/IP stack, the web server process associated with the customer accesses the customer's ARWeb account and forwards the inquiry to the ARWeb process. The ARWeb process in turn forwards the inquiry to the trouble ticketing server, which retrieves from the database engine all information needed to respond to the inquiry. The trouble ticketing server then delivers the requested information, via the network services TCP/IP stack (Sx), to the ARWeb process and eventually to the appropriate web server process, which in turn provides the information to the customer through the web interface.

When the customer wants to access network health information in the network analyzer server, the customer is allowed to access the network analyzer directly, bypassing the web server altogether. The network analyzer, which is configured with Concord Communications' "Network Health" application, maintains a unique customer account for each customer subscribing to the network management service. When a customer submits an inquiry to the network analyzer, the customer must enter a user name and password identifying the appropriate customer account in the network analyzer. The server receives the inquiry, along with the user name and password, and gathers the information needed to respond to the inquiry. The network analyzer server then delivers the requested information directly to the customer, through the firewall, bypassing the web server. Alternatively, the web server 34 may run a "Network Health" process for each customer, and all network health inquiries may be handled by the web server through the customer-specific TCP/IP stacks (S1 ... Sn) and the network services TCP/IP stack (Sx).

The web server also stores a "cron.script" file for each customer. This file contains scripts that are used to instruct the automated report server to generate trouble ticketing reports for the customer. The web server

periodically (*e.g.*, once per day) launches the "cron.script" file to run the scripts, which in turn invoke file transfer protocol (ftp) processes that transfer information from the database engine to the automated reporting server. The automated reporting server then organizes the information into customer reports. Using ftp, the automated reporting server delivers the reports to the appropriate web server process, which in turn stores the reports in the web server, *e.g.*, on the web server's hard disk. Upon receiving a request for the reports from the customer, the web server process retrieves the stored reports and delivers them to the user through the web interface.

Referring now to FIG. 4, the web server maintains a "web_servers" directory 100 on its hard disk to manage the files and processes needed to provide the network services to customers. Within this directory, the web server maintains a "customer" directory 102 for each customer with access to the network services; an "arweb" 104 directory, which stores the "ARWeb" application and all related files, including HTML forms, images, and an ARWeb configuration file; an "admin" directory 106, which is used to administer the Netscape "Enterprise Server" program; and an "SDMS_admin" directory 108, which is used to administer the customer-specific "web sites" discussed above. The "SDMS_admin" directory 108 itself includes three key directories, including a "bin" directory 110, which stores the scripts that are used, *e.g.*, in administering the customer specific web sites, adding a web site for a new customer, and adding a new action request; a "cgi-bin" directory 112, which stores scripts that are used to construct hypertext markup language (HTML) pages displayed via the web interface; and a "docs" directory 114, which stores certain HTML pages and images displayed in the

customer-specific web sites via the web interface, including a main menu page, discussed below.

Each "customer" directory 102 also includes several directories, including a "cgi-bin" directory 116, which maintains the "ARWeb" components associated with the corresponding customer; and a "docs" directory 118, which maintains several directories that store information related to network service menus presented to the customer through the web interface. The directories within the "docs" directory include an "AlarmWeb" directory 120, which stores the "AlarmWeb" software and related files, including HTML pages, images and a help file; a "network" directory 122, which stores an HTML page that provides, via the web interface, a menu associated with the network monitoring service; an "images" directory 124, which stores items such as logos, button images, and figures displayed in the customer-specific web site; a "reports" directory 126, which stores HTML pages associated with the automatic reporting service, report templates used by the service, and ftp commands invoked by the corresponding "cron.script" file to transfer reports from the automated report server to the web server; and an "action_request" directory 128, which stores HTML pages that are displayed through the web interface in connection with the trouble ticketing service.

Referring now to FIG. 5, the web server provides a graphical interface, or web interface, that allows each customer to access the network services with an off-the-shelf web browser. Each customer receives a customized version of the web interface via http transfers of files such as HTML pages and images from the web server. When a customer first gains access to the service provider's network, either through direct connection or through the Internet, as discussed above, the web server delivers an

HTML home page 130 to the customer's web browser. The home page 130 may include elements such as a logo 132 identifying the network service provider and a title bar 134 indicating the name under which the network services are provided. The home page 130 also includes several buttons 136, each of which allows the customer to access additional HTML pages related to one of the network services. For example, an "action request" button 136a invokes an HTML page that allows the customer to submit trouble tickets to the web server and to submit inquiries into the status of previously-submitted trouble tickets. A "network" button 136b invokes an HTML page that allows the customer to submit queries to the network monitoring service, including both the network analyzer server (Network Health) and the router management server (Spectrum). A "reports" button 136c invokes an HTML page that allows the customer to receive reports generated by the automated reporting server. Many of these web pages themselves include elements, such as buttons and selection boxes, that allow the user to access various features the network services.

Other embodiments are within the scope of the following claims. For example, other services, including human-oriented services such as telephone support and on-site support, may be provided in additional the computer-oriented services described above. Furthermore, while the invention has been described in terms of well-known hardware and software products, such as Remedy's "ARSystem," Seagate's "Crystal Info," and Concord's "Network Health" applications, other products that operate similarly may be used. Moreover, the software applications described above and/or other unmentioned applications may be used to provide network services other than those described.

What is claimed is:

1. A method for use in providing information to a customer whose computer network is administered remotely by a provider of network administration services, some of which are carried out by dedicated service machines executing special-purpose programs in a computer network maintained by the service provider, the method comprising:

presenting a graphical computer interface that allows the customer to request, via computer, information about the customer's network from any of the dedicated service machines,

retrieving the requested information from an appropriate one of the dedicated service machines, and

displaying the requested information to the customer via the graphical computer interface.

2. The method of claim 1, further comprising presenting the graphical computer interface in a format that allows viewing through an off-the-shelf browser application.

3. The method of claim 1, wherein presenting the graphical computer interface comprises executing a program on a network server computer.

4. The method of claim 3, further comprising configuring the network server computer to deliver the customer's request to the appropriate one of the dedicated service machines.

5. The method of claim 3, further comprising executing one instance of the program for each customer accessing the service provider's network.

6. The method of claim 3, further comprising configuring the network server computer with a unique IP address for each customer capable of accessing the service provider's network.

7. The method of claim 6, further comprising preassigning each IP address to only one customer.

8. The method of claim 6, wherein each IP address represents a TCP/IP stack in the network server computer.

9. The method of claim 1, further comprising presenting a customer-specific version of the graphical computer interface to each customer accessing the service provider's network.

10. The method of claim 1, wherein the network administration services include a trouble ticketing service.

11. The method of claim 1, wherein the network administration services include a network monitoring service.

12. An executable program, tangibly fixed in a storage medium, for use in providing information to a customer whose computer network is administered remotely by a provider of network administration services, some of which are carried out by dedicated service machines executing special-purpose programs in a computer network maintained by the service provider, the executable program comprising instructions that, when executed by a computer in the service provider's network, enable the computer to:

present a graphical computer interface that allows the customer to request, via computer, information about the customer's network from any of the dedicated service machines,

retrieve the requested information from an appropriate one of the dedicated service machines, and

display the requested information to the customer via the graphical computer interface.

13. The program of claim 12, wherein the graphical computer interface is presented in a format that allows viewing through an off-the-shelf browser application.

14. The program of claim 12, wherein the computer comprises a network server computer.

15. The program of claim 12, wherein the computer is configured to deliver the customer's request to the appropriate one of the dedicated service machines.

16. The program of claim 12, wherein the computer executes one instance of the executable program for each customer accessing the service provider's network.

17. The program of claim 12, wherein the computer is configured with a unique IP address for each customer capable of accessing the service provider's network.

18. The program of claim 17, wherein each IP address is preassigned to only one customer.

19. The program of claim 17, wherein each IP address represents a TCP/IP stack in the computer.

20. The program of claim 12, wherein a customer-specific version of the graphical computer interface is presented to each customer accessing the service provider's network.

21. The program of claim 12, wherein the network administration services include a trouble ticketing service.

22. The program of claim 12, wherein the network administration services include a network monitoring service.

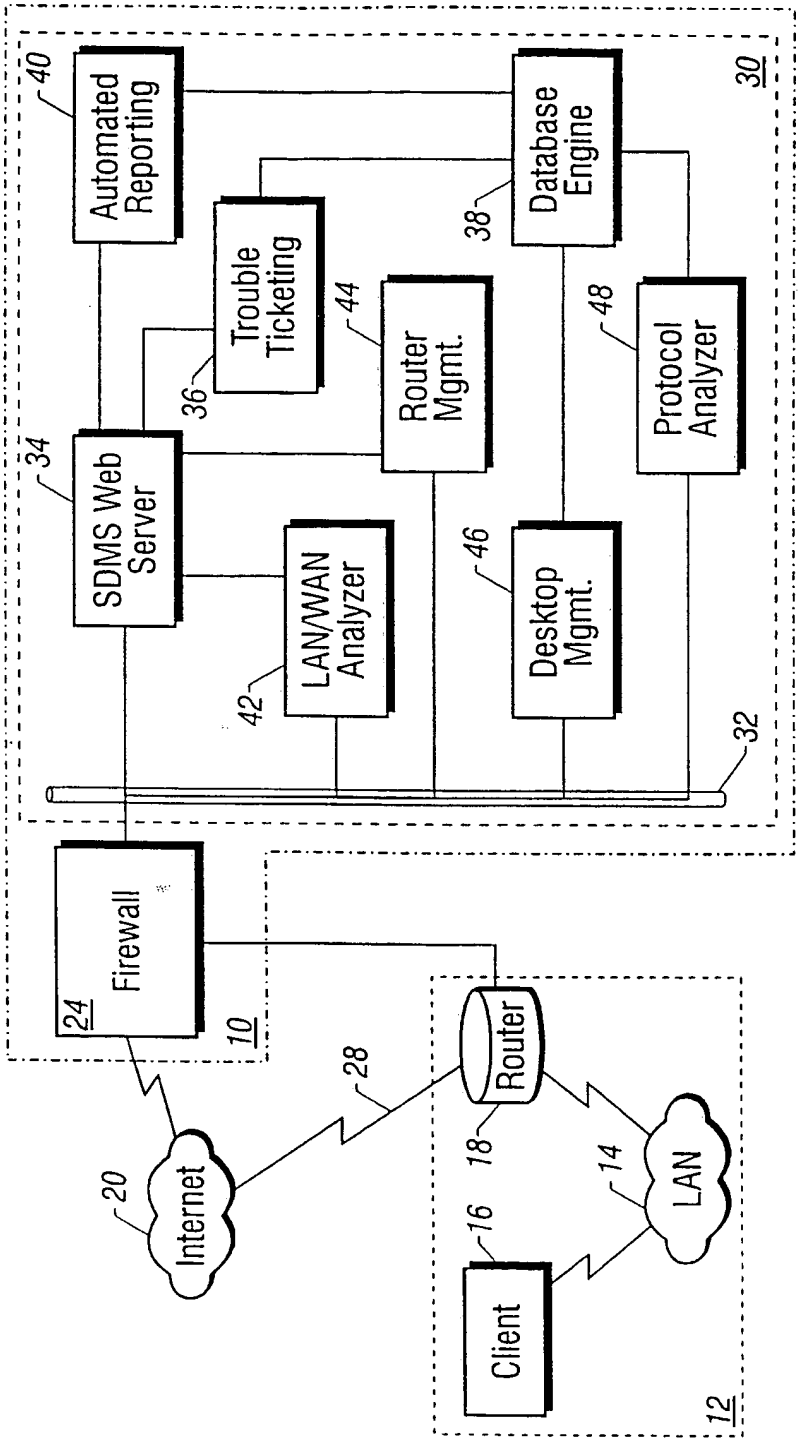

Automated Reporting
40
Database Engine
38
30
Trouble Ticketing
36
Router Mgmt.
44
Protocol Analyzer
48
SDMS Web Server
34
LAN/WAN Analyzer
42
Desktop Mgmt.
46
32
Firewall
24
10
Router
18
28
Internet
20
LAN
14
16
Client
12

Figure 1

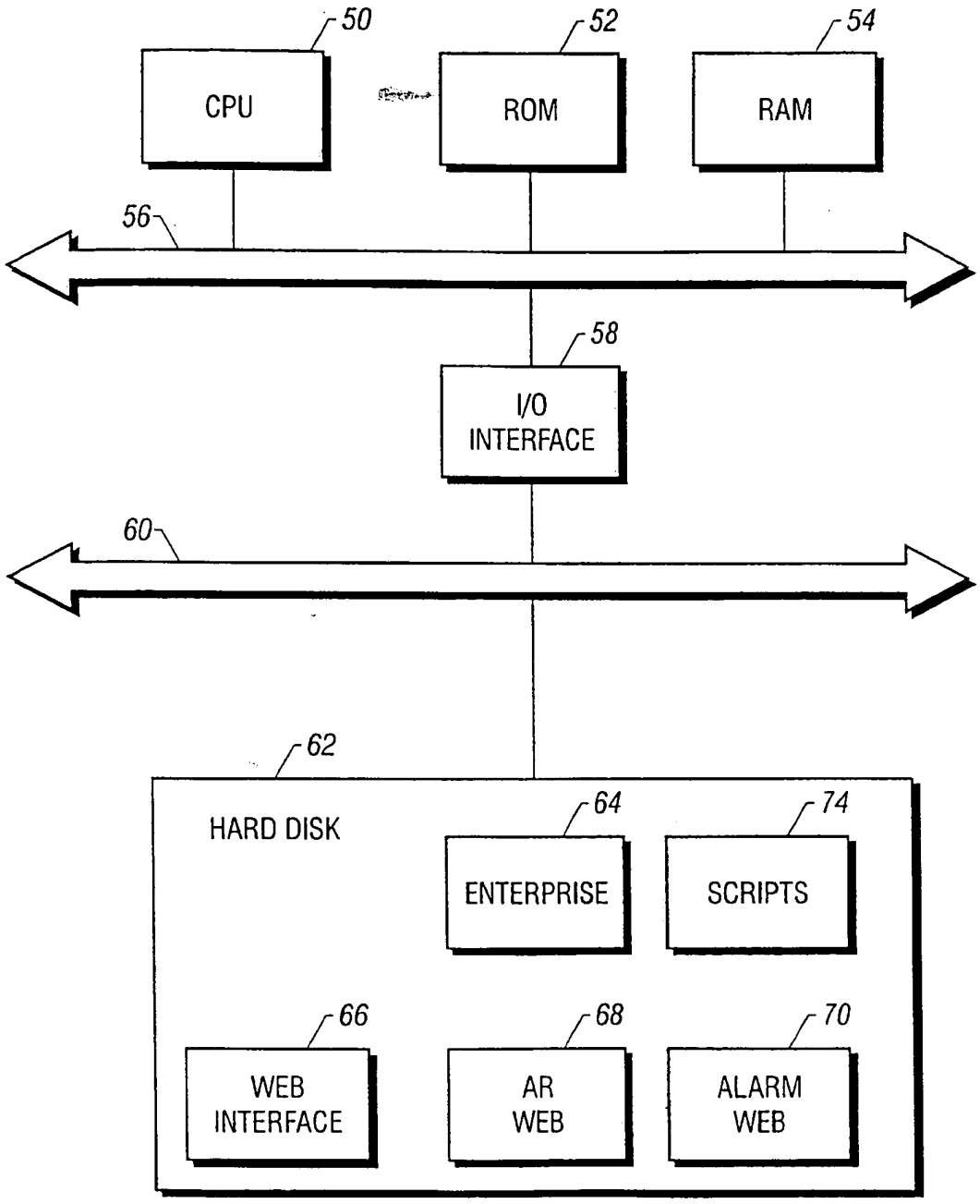

50
52
54
CPU
ROM
RAM
56
58
I/O
INTERFACE
60
62
HARD DISK
64
74
ENTERPRISE
SCRIPTS
66
68
70
WEB
INTERFACE
AR
WEB
ALARM
WEB

Figure 2

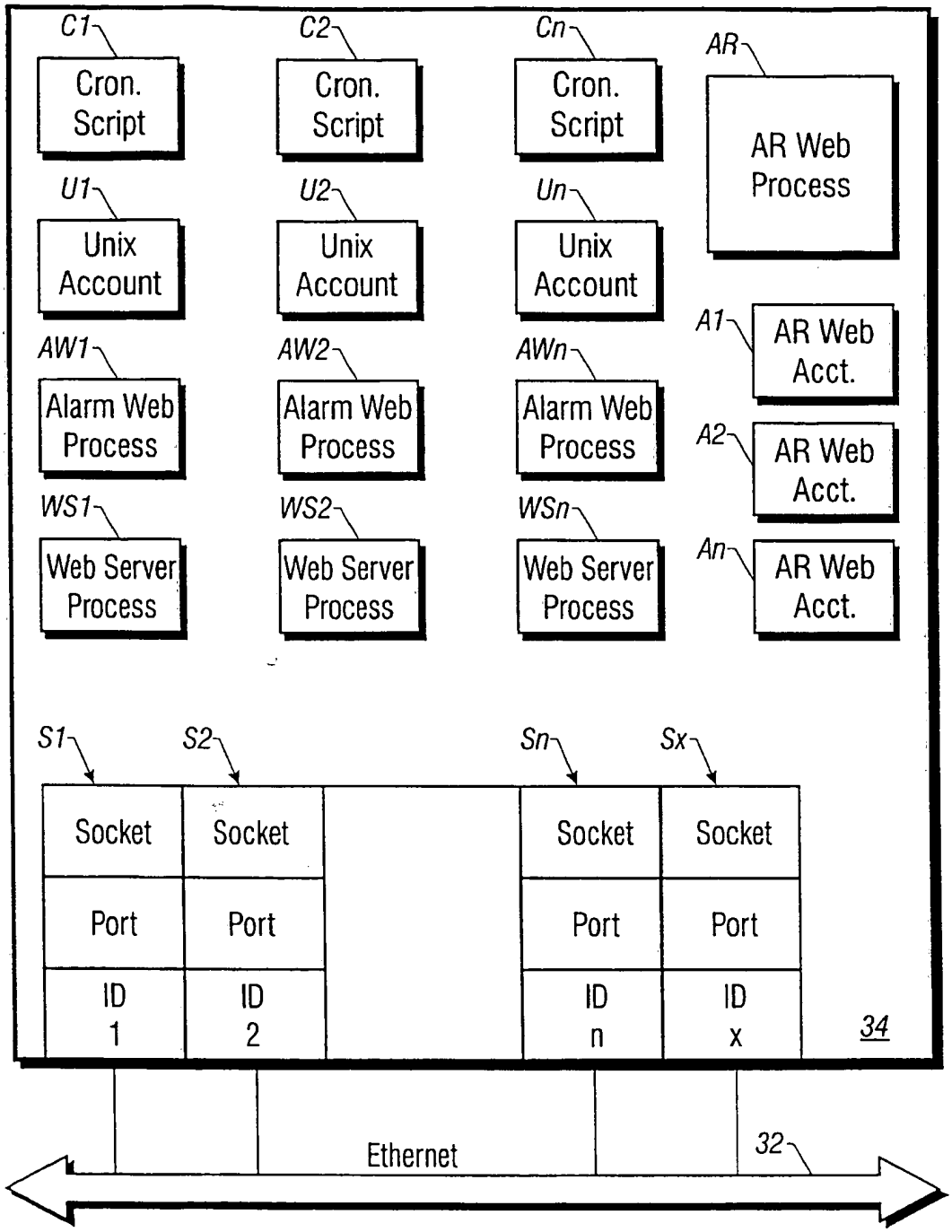

C1
Cron. Script
C2
Cron. Script
Cn
Cron. Script
AR
AR Web Process
U1
Unix Account
U2
Unix Account
Un
Unix Account
A1
AR Web Acct.
AW1
Alarm Web Process
AW2
Alarm Web Process
AWn
Alarm Web Process
A2
AR Web Acct.
WS1
Web Server Process
WS2
Web Server Process
WSn
Web Server Process
An
AR Web Acct.
S1
S2
Sn
Sx
Socket
Port
ID 1
ID 2
ID n
ID x
34
Ethernet
32

Figure 3

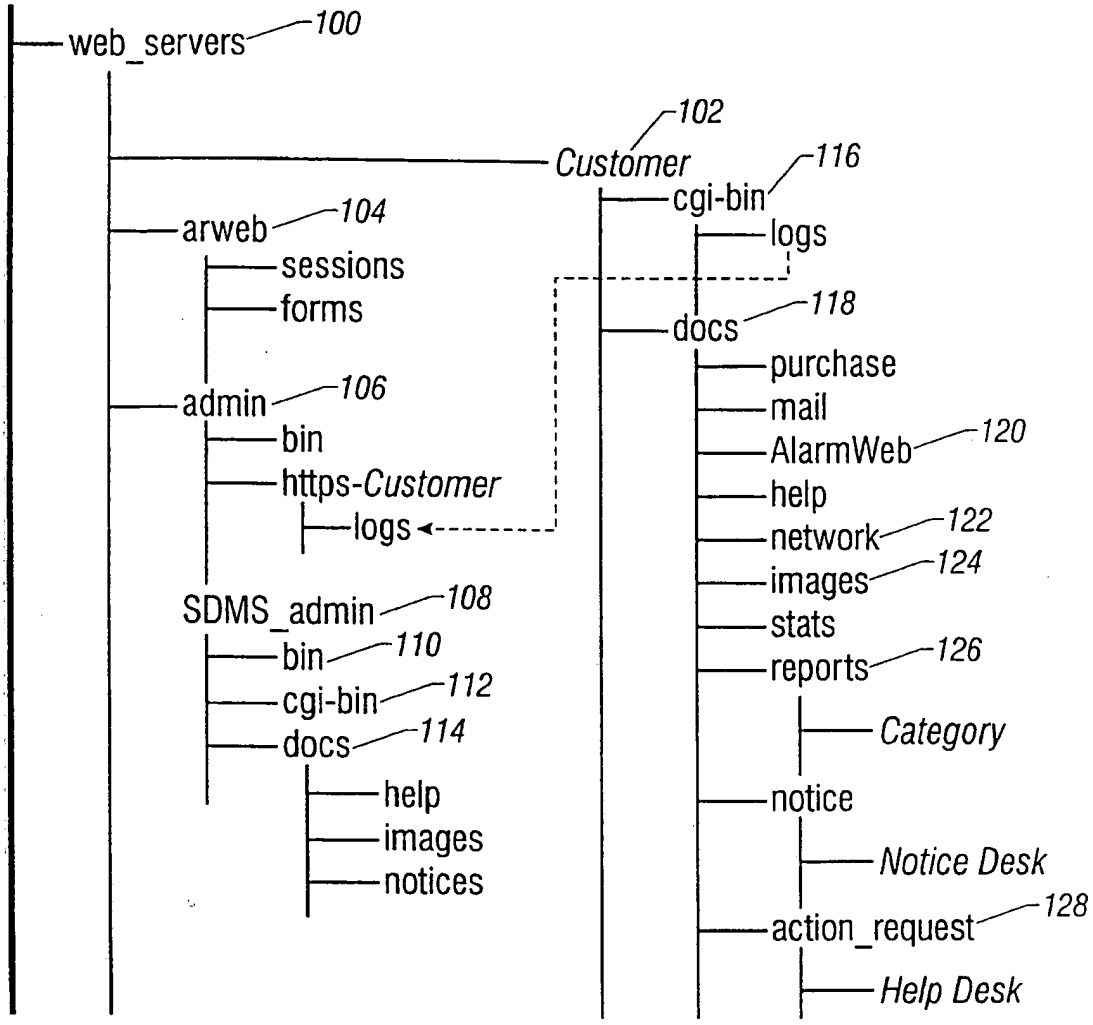

web_servers
100
Customer
102
arweb
104
sessions
forms
admin
106
bin
https-Customer
logs
SDMS_admin
108
bin
110
cgi-bin
112
docs
114
help
images
notices
cgi-bin
116
logs
docs
118
purchase
mail
AlarmWeb
120
help
network
122
images
124
stats
reports
126
Category
notice
Notice Desk
action_request
128
Help Desk

Figure 4

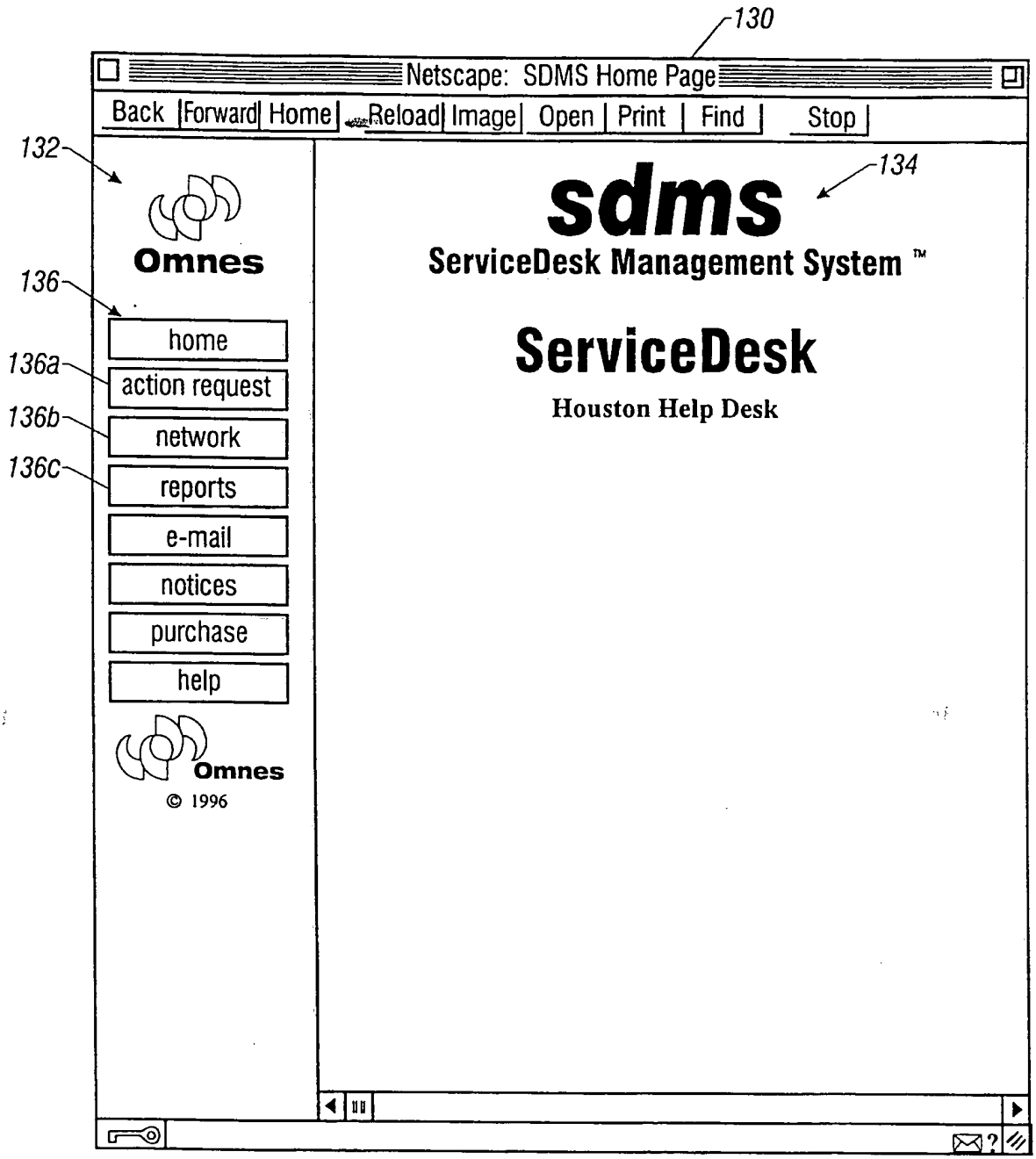

130
Netscape: SDMS Home Page
Back
Forward
Home
Reload
Image
Open
Print
Find
Stop
132
Omnes
136
home
136a
action request
136b
network
136c
reports
e-mail
notices
purchase
help
Omnes
© 1996
134
sdms
ServiceDesk Management System ™
ServiceDesk
Houston Help Desk

Figure 5